

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 1月28日
Date of Application:

出願番号 特願2003-018309
Application Number:

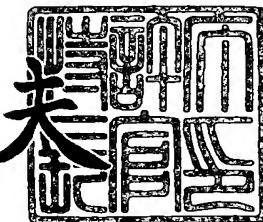
[ST. 10/C] : [JP2003-018309]

出願人 インターナショナル・ビジネス・マシーンズ・コーポレーション
Applicant(s):

2003年12月 2日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 JP9020222

【提出日】 平成15年 1月28日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 13/10

【発明者】

【住所又は居所】 神奈川県大和市下鶴間1623番地14 日本アイ・ビー
ー・エム株式会社 大和事業所内

【氏名】 佐々木 健

【発明者】

【住所又は居所】 神奈川県大和市下鶴間1623番地14 日本アイ・ビー
ー・エム株式会社 大和事業所内

【氏名】 伊藤 貴志子

【発明者】

【住所又は居所】 神奈川県大和市下鶴間1623番地14 日本アイ・ビー
ー・エム株式会社 大和事業所内

【氏名】 美根 宏昭

【特許出願人】

【識別番号】 390009531

【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレ
ーション

【代理人】

【識別番号】 100086243

【弁理士】

【氏名又は名称】 坂口 博

【代理人】

【識別番号】 100091568

【弁理士】

【氏名又は名称】 市位 嘉宏

【代理人】

【識別番号】 100108501

【弁理士】

【氏名又は名称】 上野 剛史

【復代理人】

【識別番号】 100104880

【弁理士】

【氏名又は名称】 古部 次郎

【選任した復代理人】

【識別番号】 100118201

【弁理士】

【氏名又は名称】 千田 武

【手数料の表示】

【予納台帳番号】 081504

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9706050

【包括委任状番号】 9704733

【包括委任状番号】 0207860

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンピュータシステム、コンピュータ装置、記憶装置のデータ保護方法、およびプログラム

【特許請求の範囲】

【請求項 1】 ユーザの環境で動作するユーザ領域と、書き込み保護を必要とするアプリケーションが格納される隠蔽された領域とを有する記憶装置と、前記記憶装置の前記隠蔽された領域に格納される前記アプリケーションを展開可能に構成され、擬似的なディスクスペースを提供するメモリとを含むコンピュータシステム。

【請求項 2】 前記記憶装置は、PARTIES (Protected Area Run Time Interface Extension Services)の仕様、もしくはそれに準ずる規格仕様を満たし、前記隠蔽された領域はPARTIESパーティションであることを特徴とする請求項1記載のコンピュータシステム。

【請求項 3】 前記記憶装置は、BIOSのサポートにより前記隠蔽された領域からのブートが実行されることを特徴とする請求項1記載のコンピュータシステム。

【請求項 4】 データを保持する記憶装置を備えたコンピュータシステムであって、

前記記憶装置は、
ユーザの環境で動作する領域である第1のパーティションと、
前記第1のパーティションとは別の領域であって、書き込み保護を必要とする
アプリケーションが格納される第2のパーティションとを含み、

前記第2のパーティションは、前記書き込み保護を必要とするアプリケーションの中から所定のアプリケーションが実行される際に、当該所定のアプリケーションを展開可能とする空き領域を有することを特徴とするコンピュータシステム。

【請求項 5】 前記第2のパーティションは、PARTIES (Protected Area Run Time Interface Extension Services)パーティションであることを特徴とする請求項4記載のコンピュータシステム。

【請求項 6】 ユーザの環境で動作する第1の領域とユーザから隠蔽された領域である第2の領域とを形成可能な外部記憶装置を備えたコンピュータシステムであって、

前記第2の領域に格納されているアプリケーションの中から、所定のアプリケーションのブートをサポートするブートサポート手段と、

前記所定のアプリケーションに対する物主証明のための承認を行う承認手段と、

前記所定のアプリケーションが承認されたアプリケーションである場合に、所定のメモリ上の空き領域または前記第2の領域における空き領域に当該所定のアプリケーションをコピーして、擬似アプリケーションエリアを形成する擬似アプリケーションエリア形成手段と、を含み、

前記所定のアプリケーションへのアクセスは、前記擬似アプリケーションエリアに対して行われることを特徴とするコンピュータシステム。

【請求項 7】 前記擬似アプリケーションエリア形成手段は、前記所定のアプリケーションのサイズを検出し、前記所定のメモリ上の空き領域または前記第2の領域の空き領域を調べて領域を確保した後、前記擬似アプリケーションエリアを形成することを特徴とする請求項6記載のコンピュータシステム。

【請求項 8】 前記擬似アプリケーションエリア形成手段は、前記第2の領域に前記擬似アプリケーションエリアを形成する際に、前記所定のアプリケーションのサイズを検出して当該第2の領域のアンロックをB IOSに要求した後、当該擬似アプリケーションエリアを当該第2の領域に形成することを特徴とする請求項6記載のコンピュータシステム。

【請求項 9】 ユーザの環境で動作するエリアであるユーザエリアと、ユーザから保護されたエリアであるホストプロテクティッドエリアとに区別されてデータを保持する記憶装置に対してアクセスするコンピュータ装置であって、

前記ホストプロテクティッドエリアからのブートをサポートすると共に、当該ホストプロテクティッドエリアにあるアプリケーションに対する物主証明のための承認をサポートするB IOSと、

前記ホストプロテクティッドエリアにある前記アプリケーションを他のメモリ

の空き領域または当該ホストプロテクティッドエリアの空き領域にコピーして擬似アプリケーションエリアを生成するアプリケーションアクセスモジュールとを含むコンピュータ装置。

【請求項 10】 前記B IOSは、秘密鍵の管理および/または前記ホストプロテクティッドエリアのアクセス管理を行うことを特徴とする請求項9記載のコンピュータ装置。

【請求項 11】 前記アプリケーションアクセスモジュールは、前記ホストプロテクティッドエリアにある前記アプリケーションがライトプロテクトされたものであるかどうかを判断すると共に、当該アプリケーションへのアクセスが行われる場合に、前記擬似アプリケーションエリアにアクセスすることを特徴とする請求項9記載のコンピュータ装置。

【請求項 12】 ユーザの環境で動作する第1のエリアとユーザから隠蔽された領域である第2のエリアとを有してデータを保持する記憶装置のデータ保護方法であって、

前記第2のエリアにある所定のアプリケーションをブートする際に、前記第2のエリアをアンロックするステップと、

アンロックされた前記第2のエリアから前記所定のアプリケーションを読み込むステップと、

アンロックされた前記第2のエリアをロックするステップと、

読み込まれた前記所定のアプリケーションを、他のメモリ上の空き領域に形成された擬似アプリケーションエリアにコピーするステップと、

前記擬似アプリケーションエリアから前記所定のアプリケーションをブートするための最初のコードを読み込むステップと

を含む記憶装置のデータ保護方法。

【請求項 13】 前記第2のエリアにある所定のアプリケーションが物主により承認されたアプリケーションか否かを判断するステップと、

前記所定のアプリケーションが承認されたアプリケーションである場合に、ライトプロテクトが必要かどうかを検出するステップと

を更に含む請求項12記載の記憶装置のデータ保護方法。

【請求項 14】 ユーザの環境で動作する第1のエリアとユーザから隠蔽された領域である第2のエリアとを有してデータを保持する記憶装置のデータ保護方法であって、

前記第2のエリアにある承認されたアプリケーションをブートする際に、前記第2のエリアをアンロックするステップと、

アンロックされた前記第2のエリアから前記アプリケーションを読み込むステップと、

読み込まれた前記アプリケーションを、前記第2のエリアにおける空き領域に設けられた擬似アプリケーションエリアにコピーするステップと、

前記擬似アプリケーションエリアから前記アプリケーションをブートするための最初のコードを読み込むステップと

を含む記憶装置のデータ保護方法。

【請求項 15】 前記最初のコードを読み込むステップは、ディスクアクセスプログラムのアクセス範囲を、前記アプリケーションをコピーしたエリアに向けることにより、前記擬似アプリケーションエリアから当該最初のコードを読み込むことを特徴とする請求項14記載の記憶装置のデータ保護方法。

【請求項 16】 ユーザの動作環境である第1のエリアとユーザから隠蔽された領域である第2のエリアとを有する記憶装置を備えたコンピュータに、

前記第2のエリアに対するアンロックを要求する機能と、

アンロックされた前記第2のエリアから、物主により承認され且つライトプロテクトが必要であるアプリケーションを読み込む機能と、

アンロックされた前記第2のエリアに対するロックを要求する機能と、

読み込まれた前記アプリケーションを、前記記憶装置とは異なるメモリ上の空き領域に設けられる擬似アプリケーションエリアにコピーする機能と

を実現させるプログラム。

【請求項 17】 前記コンピュータに、

前記擬似アプリケーションエリアから前記アプリケーションをブートする機能を更に実現させる請求項16記載のプログラム。

【請求項 18】 ユーザの動作環境である第1のエリアとユーザから隠蔽さ

れた領域である第2のエリアとを有する記憶装置を備えたコンピュータに、
前記第2のエリアに対するアンロックを要求する機能と、
アンロックされた前記第2のエリアから、物主により承認され且つライトプロ
テクトが必要であるアプリケーションを読み込む機能と、
読み込まれた前記アプリケーションを、前記第2のエリアの空き領域に設けら
れる擬似アプリケーションエリアにコピーする機能と、
前記アプリケーションに対するアクセスを前記擬似アプリケーションエリアに
向ける機能と
を実現させるプログラム。

【請求項19】 前記アプリケーションに対するアクセスを前記擬似アプリ
ケーションエリアに向ける機能は、当該アプリケーションに対するアクセステー
ブルのアドレスをコピー先のアドレスとする請求項18記載のプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ハードディスクドライブ(HDD)などの記憶装置を備えたコンピュ
ータシステム等に係り、より詳しくは、所定のユーザ環境とユーザから隠蔽され
た領域とを有する記憶装置を備えたコンピュータシステム等に関する。

【0002】

【従来の技術】

従来、業界標準規格であるATA(AT Attachment)/ATAPI(Advanced Tech
nology Attachment Packet Interface)-5の仕様をサポートするハードディス
クドライブ(HDD:Hard Disk Drive)の機能を使用し、ANSI(American Nat
ional Standards Institute)のスタンダードであるPARTIES(Protected A
rea Run Time Interface Extension Services)のアーキテクチャを用いて、HD
Dの中にユーザから隠蔽した領域、即ち、ユーザから自由にアクセスするこ
とができない領域を作成することが可能である。

【0003】

図7は、HDDにおけるPARTIESの機能を説明するための図であり、H

DDの領域を横に輪切りにしたイメージで表現している。ここでは、擬似的な最大領域である"Max"の値を定義し、通常のコマンドでは、この"Max"までが領域として与えられ、OSは、"Start"から"Max"までを使用領域としている。この"Max"の値からHDDにおける本当の最大領域である"Native Max"までがPARTIESパーティション(PARTIES Partition)である。このPARTIESパーティションにて規格が決まっている/もしくは定義されている"Boot Engineering Extension Record"には、PARTIESパーティションに入っている情報が格納されており、ここを参照することで、PARTIESパーティションに対する種々の機能を使用することができる。

【0004】

このPARTIESの仕様で想定されている使い方としては、通常、フロッピーディスクなどのリムーバルメディアからブートされるときにあてがわれるAドライブを、PARTIESパーティションからブートするときにもあてがい、例えば、BIOS (Basic Input/Output System)のInterrupt 40というリムーバルメディアに対するBIOSコールを利用して、PARTIESパーティションに対するアクセスを行うサービスが存在する。即ち、PARTIESパーティションからブートして、Aドライブが見え、通常の領域であるユーザパーティションをCドライブとして見せるように構成している。これによって、PARTIESのエリアにOSのプリロードイメージを格納しておき、ここからのリカバリを可能としたり、BIOSセットアップである、ハードウェアの設定、パスワードの設定、ブートシーケンスの記載等に必要な情報を、ROMに代わって格納し、例えば、グラフィカルなユーザインターフェースを用いたユーザによるセットアップ作業を可能としている。また、ブート(起動)プログラムを入れておき、ここからシステムの診断を行うこともPARTIESの仕様として想定されている。

【0005】

また、本件発明とは直接関係しないが、ハードディスクに対するデータ保護の従来技術として、入力されたパスフレーズをハッシュ関数によって処理し、HDD内のデータを保護する技術がある(例えば、特許文献1参照。)。

【0006】

【特許文献1】

特開2001-306266号公報(第3頁、図1)

【0007】**【発明が解決しようとする課題】**

このような、ATA/ATAPI-5、およびANSI PARTIESを用いて、書き込み保護したいPARTIESのパーティションにおける書き込みを保護し、PARTIESパーティションに導入されているアプリケーションによるデータの変更を制限することが可能である。しかしながら、PARTIESパーティション上のアプリケーションを実行する場合、アプリケーション自身がPARTIESのパーティションにあることから、読み込みや書き込みの制限を加えることは、現状の技術だけでは困難である。

【0008】

ここで、PARTIESパーティション上のアプリケーションの内容は、物主(アプリケーションを作成して書き込んだオーナー)の証明のために、ハッシュ関数などのBIOS内のプライベートキーを用いて承認が行われている。そのため、アプリケーションの内容が変更されると、即ち、PARTIESパーティション上のアプリケーションを実行して書き込みが行われてしまうと、承認されていない不正なアプリケーションとみなされ、アプリケーションの起動時にエラーとなってしまう。HDDでは、あるエリアだけを書き込み保護する機能は存在せず、PARTIES用のパーティションを開発する場合に、書き込みの制限を意識して書き込み保護を実現する必要がある。

【0009】

本発明は、以上のような技術的課題を解決するためになされたものであって、その目的とするところは、例えばHDD等の記憶装置において、ユーザから隠蔽された領域に格納されたデータに対する書き込み制限を実現することにある。

また他の目的は、例えば、HDDにおけるPARTIESパーティション上のアプリケーション側でPARTIESパーティション用にアプリケーションを変更、開発することなく、書き込みを制限することにある。

更に他の目的は、例えば、HDDにおけるPARTIESパーティション上の

アプリケーションに対して、予期しない書き込みに対する対応を特別に行わなくとも、これらの書き込みに対する対応を可能とすることにある。

また更に他の目的は、PARTIESの仕様の利用範囲を拡張することにある。

【0010】

【課題を解決するための手段】

かかる目的のもと、本発明が適用されるコンピュータシステムは、ATA/ATAPI-5、および、ANSI PARTIESを用いて書き込み保護したいPARTIESのパーティションの書き込みを保護し、PARTIESパーティションに導入されているアプリケーションによるデータの変更を制限している。即ち、本発明が適用されるコンピュータシステムは、例えば、PARTIESの仕様、もしくはそれに準ずる規格仕様を満たし、ユーザの環境で動作するユーザ領域と、書き込み保護を必要とするアプリケーションが格納される隠蔽された領域(例えば、PARTIESパーティション)とを有する記憶装置と、この記憶装置の隠蔽された領域に格納されるアプリケーションを展開可能に構成され、擬似的なディスクスペースを提供するメモリとを含む。ここで、この記憶装置は、BIOSのサポートにより隠蔽された領域からのブートが実行されることを特徴とすることができる。

【0011】

また、本発明は、データを保持する記憶装置を備えたコンピュータシステムであって、この記憶装置は、ユーザの環境で動作する領域である第1のパーティション(ユーザエリア)と、この第1のパーティションとは別の領域であって、書き込み保護を必要とするアプリケーションが格納される第2のパーティション(PARTIESパーティション、ホストプロテクティッドエリア)とを含み、この第2のパーティションは、書き込み保護を必要とするアプリケーションの中から所定のアプリケーションが実行される際に、この所定のアプリケーションを展開可能とする空き領域を有することを特徴とする。

【0012】

一方、本発明は、ユーザの環境で動作する第1の領域とユーザから隠蔽された

領域である第2の領域とを形成可能な外部記憶装置を備えたコンピュータシステムであって、ブートサポート手段により、第2の領域に格納されているアプリケーションの中から、所定のアプリケーションのブートをサポートし、承認手段により、この所定のアプリケーションに対する物主証明のための承認を行い、この所定のアプリケーションが承認されたアプリケーションである場合に、擬似アプリケーションエリア形成手段により、所定のメモリ上の空き領域または前記第2の領域における空き領域にこの所定のアプリケーションをコピーして、擬似アプリケーションエリアを形成している。そして、この所定のアプリケーションへのアクセスは、擬似アプリケーションエリアに対して行われることを特徴とすることができる。

【0013】

ここで、この擬似アプリケーションエリア形成手段は、所定のアプリケーションのサイズを検出し、所定のメモリ上の空き領域または第2の領域の空き領域を調べて領域を確保した後、擬似アプリケーションエリアを形成することを特徴としている。また、この擬似アプリケーションエリア形成手段は、第2の領域に擬似アプリケーションエリアを形成する際に、所定のアプリケーションのサイズを検出して第2の領域のアンロックをB IOSに要求した後、擬似アプリケーションエリアを第2の領域に形成することを特徴とすることができる。

【0014】

他の観点から捉えると、本発明は、ユーザの環境で動作するエリアであるユーザエリア(User Area)と、ユーザから保護されたエリアであるホストプロテクティッドエリア(Host Protected Area)とに区別されてデータを保持するHDD等の記憶装置に対してアクセスするコンピュータ装置であって、ホストプロテクティッドエリアからのブートをサポートすると共に、このホストプロテクティッドエリアにあるアプリケーションに対する物主証明のための承認をサポートするB IOS(Basic Input/Output System)と、ホストプロテクティッドエリアにあるアプリケーションを他のメモリの空き領域またはホストプロテクティッドエリアの空き領域にコピーして擬似アプリケーションエリアを生成するアプリケーションアクセスモジュールとを含む。

【0015】

ここで、このB IOSは、秘密鍵の管理および/またはホストプロテクティッドエリアのアクセス管理を行うことを特徴とする。また、アプリケーションアクセスモジュールは、ホストプロテクティッドエリアにあるアプリケーションがライトプロテクトされたものであるかどうかを判断すると共に、このアプリケーションへのアクセスが行われる場合に、擬似アプリケーションエリアにアクセスすることを特徴とすることができます。

【0016】

更に、本発明は、ユーザの環境で動作する第1のエリアとユーザから隠蔽された領域である第2のエリアとを有してデータを保持する記憶装置のデータ保護方法であって、第2のエリアにある所定のアプリケーションをブートする際に、この第2のエリアにある所定のアプリケーションが物主により承認されたアプリケーションか否かを判断するステップと、所定のアプリケーションが承認されたアプリケーションである場合にライトプロテクトが必要かどうかを検出するステップと、この第2のエリアをアンロックするステップと、アンロックされたこの第2のエリアから所定のアプリケーションを読み込むステップと、アンロックされた第2のエリアをロックするステップと、読み込まれた所定のアプリケーションを、他のメモリ上の空き領域に形成された擬似アプリケーションエリアにコピーするステップと、擬似アプリケーションエリアから所定のアプリケーションをブートするための最初のコードを読み込むステップとを含む。

【0017】

他の観点から捉えると、本発明が適用される記憶装置のデータ保護方法は、第2のエリアにある承認されたアプリケーションをブートする際に、この第2のエリアをアンロックするステップと、アンロックされた第2のエリアからアプリケーションを読み込むステップと、読み込まれたアプリケーションを、第2のエリアにおける空き領域に設けられた擬似アプリケーションエリアにコピーするステップと、この擬似アプリケーションエリアからアプリケーションをブートするための最初のコードを読み込むステップとを含む。ここで、この最初のコードを読み込むステップは、ディスクアクセスプログラムのアクセス範囲を、アプリケ

ションをコピーしたエリアに向けることにより、擬似アプリケーションエリアから最初のコードを読み込むことを特徴とすれば、書き込み保護したいPARTIESのパーティションの書き込み保護を実現できる点から好ましい。

【0018】

ここで、本発明は、コンピュータに所定の機能を実現させるプログラムとして把握することができる。即ち、本発明が適用されるプログラムは、ユーザの動作環境である第1のエリアとユーザから隠蔽された領域である第2のエリアとを有する記憶装置を備えたコンピュータに、第2のエリアに対するアンロックを要求する機能と、アンロックされた第2のエリアから、物主により承認され且つライトプロテクトが必要であるアプリケーションを読み込む機能と、アンロックされた第2のエリアに対するロックを要求する機能と、読み込まれたアプリケーションを、記憶装置とは異なるメモリ上の空き領域に設けられる擬似アプリケーションエリアにコピーする機能と、擬似アプリケーションエリアからアプリケーションをブートする機能とを実現させる。

【0019】

また、本発明が適用されるプログラムは、コンピュータに、第2のエリアに対するアンロックを要求する機能と、アンロックされた第2のエリアから、物主により承認され且つライトプロテクトが必要であるアプリケーションを読み込む機能と、読み込まれたアプリケーションを、第2のエリアの空き領域に設けられる擬似アプリケーションエリアにコピーする機能と、例えばアプリケーションに対するアクセステーブルのアドレスをコピー先のアドレスとして、アプリケーションに対するアクセスを擬似アプリケーションエリアに向ける機能とを実現させる。

【0020】

尚、これらのプログラムとしては、コンピュータを顧客に対して提供する際に、装置の中にインストールされた状態にて提供される場合の他、コンピュータに実行させるプログラムをコンピュータが読み取可能に記憶した記憶媒体にて提供する形態が考えられる。この記憶媒体としては、例えばCD-ROM媒体等が該当し、CD-ROM読み取り装置等によってプログラムが読み取られて実行される。ま

た、これらのプログラムは、例えば、プログラム伝送装置によってネットワークを介して提供される形態がある。このプログラム伝送装置としては、例えば、ホスト側のサーバに設けられ、プログラムを格納するメモリと、ネットワークを介してプログラムを提供するプログラム伝送手段とを備えている。

【0021】

【発明の実施の形態】

以下、添付図面に示す実施の形態に基づいて本発明を詳細に説明する。

[実施の形態1]

図1は、実施の形態1におけるコンピュータシステムの全体構成を示した図である。図1に示すコンピュータシステムは、大きくハードウェア10とソフトウェア20の構成要素に分けることができる。ここで、「システム」とは、複数の装置(機能)が論理的に集合した物をいい、各構成の装置(機能)が同一筐体中にあるか否かを問うものではない。従って、例えば、これらの構成要素が1つの装置にまとまって1つの取引対象となる場合もあり、また、特定の要素が別筐体として単体で扱われる場合もある。実施の形態2(後述)に示すコンピュータシステムも「システム」の考え方は同様である。

【0022】

ハードウェア10としては、OS(Operating System)/ユーザデータを保持するための不揮発性記憶装置であるHDD(Hard Disk Drive)11、PARTIES(Protected Area Run Time Interface Extension Services)パーティションをコピーするための記憶装置であるメモリ(Memory)12を備えている。HDD11は、PARTIESの仕様を満たすために、ATA(AT Attachment)/ATAPI(Advanced Technology Attachment Packet Interface)-5の仕様をサポートしている。このHDD11は、ユーザが自由にアクセスできる領域として、即ち、ユーザの環境で動作する領域(通常のパーティション)と、システムパーティションとして、ユーザから保護された、ユーザから隠蔽された領域であるPARTIESパーティションとを備えている。また、メモリ12は、RAMなどで構成され、擬似PARTIESアプリケーションエリア(後述)として使用される。

【0023】

ソフトウェア20としては、コンピュータシステムに接続されている各種デバイスを制御するBIOS (Basic Input/Output System) 21、コンピュータシステムを提供する物主(システムベンダー：System Vendor)により提供された、ユーザから保護された領域(PARTIES Area)であるホストプロテクティッドエリア(Host Protected Area) 22、ユーザの環境で動作する領域であるユーザエリア(User Area) 24を有している。ホストプロテクティッドエリア 22には、ブート(Boot)可能なアプリケーションであり、システムベンダーにより提供されるサービスであるPARTIESアプリケーション(PARTIES Application) 23が格納されている。

【0024】

また、ソフトウェア20には、PARTIESアプリケーション23がライトプロテクト(Write Protect)されたものであるかどうかを判断するPARTIESアプリケーションアクセスモジュール(PARTIES Application Access Module) 25、PARTIESアプリケーション23をメモリ12上にコピーしたワークエリアである擬似PARTIESアプリケーションエリア26を有している。PARTIESアプリケーションアクセスモジュール25は、上記の役割の他に、メモリ12上の空き領域を調べて確保する役割、PARTIESアプリケーション23をメモリ12にコピーし、擬似PARTIESアプリケーションエリア26を作る役割、PARTIESアプリケーション23へのアクセスが行われる場合、擬似PARTIESアプリケーションエリア26にアクセスする役割、を担っている。

【0025】

BIOS 21は、PARTIESアプリケーション23の仕様をサポートすると共に、PARTIESパーティションからのブートをサポートしている。また、PARTIESアプリケーション23に対する、物主証明のための承認をサポートする機能の他、秘密鍵を管理する機能も備えている。更に、ホストプロテクティッドエリア22のアクセス管理を実行する機能も備えている。

【0026】

次に、PARTIESのパーティションにおける書き込み保護について説明す

る。

図2は、実施の形態1における書き込み保護方法を説明するための図である。ここでは、ブートが行われる場合、プロテクションされているセキュアなエリアであるPARTIESパーティションを有するHDD11に対して、BIOS21から、ディスクアクセスプログラムであるINT40(Interrupt40)に則ってディスクアクセスが実行される。HDD11の中にユーザから隠蔽した領域としてPARTIESによって作成されるPARTIESパーティションは、一旦、ユーザの環境からブートした後は、通常そのエリアについては触ることが出来ない。即ち、セキュアードなパーティションとして、ユーザの環境からはデータを壊されることなく、データアクセスがなされることなく、その結果、ウィルスの進入等を防ぐことも可能である。図2に示す例では、このPARTIESパーティションに、ヘッダであるBEEERと、PARTIESアプリケーションとしてPSA0～PSA5とが格納されている。

【0027】

このPARTIESパーティションには、システムベンダー(物主)により提供されるサービスであって、ユーザから保護されなければならないアプリケーションとして、

- Diagnostic Service
- OS Recovery Service
- Restore from backup Service
- Create diagnostic diskettes Service
- Download BIOS Service
- Download Drivers Service
- Update BIOS Service
- Administrator tools

等が格納される。

【0028】

しかしながら、BIOS21の例えればINT40によってPARTIESパーティションにアクセスした場合、このPARTIESパーティションのエリアに

あるアプリケーションを走らせてしまうと、ロックできずに、通常、書き込みが可能となってしまう。PARTIESパーティションのエリアにあるアプリケーションに対しては、ブート(Boot)に際して、BIOS21の持つプライベートキーを用いてValidation(承認)が行われるが、PARTIESパーティション上のアプリケーションが変更されていると、Validationでエラーが起き、ブートすることができない。

【0029】

そこで実施の形態1では、実行しようとするアプリケーションをRAM等のメモリ12に全て展開し、擬似的なディスクスペースへのアクセスとして、PARTIESパーティションへの書き込み保護を実現する。図2に示す例では、PSA3のアプリケーションをメモリ12に一旦、展開している。このとき、例えば、メモリ12の所定の領域に格納され、ディスクアクセスプログラムのアクセステーブルには、スタートとしてメモリ12におけるPSA3'のスタートアドレス、エンドとしてメモリ12におけるPSA3'のエンドアドレスが格納されている。これによって、リードもライトも、メモリ12上のPSA3'となるよう変更される。これによって、擬似的なディスクスペースにアクセスし、PARTIESパーティションへの書き込み保護を実現している。

【0030】

図3は、実施の形態1におけるPARTIESアプリケーションのブートの流れを示したフローチャートである。PARTIESアプリケーションのブートを実行するに際して(ステップ101)、まず、BIOS21は、ホストプロテクティッドエリア22をアンロックする(ステップ102)。次に、BIOS21は、ホストプロテクティッドエリア22のアクセス機能を用意する(ステップ103)。即ち、ディスクアクセスのルーチンを用意する。その後、BIOS21は、PARTIESアプリケーション23の承認(Validation)を行う。即ち、例えばHash値によって物主による承認を受ける(ステップ104)。そして、BIOS21は、ホストプロテクティッドエリア22をロックする(ステップ105)。ここで、BIOS21では、承認されたアプリケーションか否かの判断がなされる(ステップ106)。承認されたアプリケーションではない場合には、BIOS2

1は、エラーを表示し、ブートを失敗させる(ステップ107)。ステップ106で承認されたアプリケーションである場合には、ステップ108に移行する。

【0031】

PARTIESアプリケーションアクセスモジュール25は、PARTIESアプリケーション23のライトプロテクト(Write Protect)が必要かどうかを検出する(ステップ108)。そして、PARTIESアプリケーションアクセスモジュール25は、PARTIESアプリケーション23のサイズ検出がなされる(ステップ109)。その後、PARTIESアプリケーションアクセスモジュール25は、メモリ12の領域を確保し、擬似PARTIESアプリケーションエリア26を作る(ステップ110)。そして、PARTIESアプリケーションアクセスモジュール25は、BIOS21にホストプロテクティッドエリア22のアンロックを要求し(ステップ111)、PARTIESアプリケーションアクセスモジュール25は、メモリ12上に確保した擬似PARTIESアプリケーションエリア26にPARTIESアプリケーション23をコピーする(ステップ112)。その後、PARTIESアプリケーションアクセスモジュール25は、BIOS21にホストプロテクティッドエリア22のロックを要求する(ステップ113)。これによって、PARTIESパーティション上にあるPARTIESアプリケーション23の書き込み保護が可能となる。

【0032】

そして、PARTIESアプリケーションアクセスモジュール25は、擬似PARTIESアプリケーションエリア26に対するアクセス機能(ディスクアクセスプログラム)を用意し、BIOS21によって用意されたディスクアクセスプログラムと入れ替える(ステップ114)。その後、BIOS21は、ブートのための最初のコードであるイニシャルプログラムローダを擬似PARTIESアプリケーションエリア26から読み込み(ステップ115)、BIOS21によるPARTIESアプリケーション23のブートが実行される(ステップ116)。

【0033】

以上、詳述したように、本実施の形態では、HDD11における、実行しようとするアプリケーションを、全てRAM等のメモリ12上に展開し、BIOS2

1によって、擬似的なディスクスペースへアクセスするように構成した。これによって、PARTIESパーティションへの書き込み保護を実現した状態にて、通常のアプリケーションをPARTIESパーティション用のアプリケーションとして使用することが可能となる。

【0034】

[実施の形態2]

実施の形態1では、PARTIESアプリケーション23を、RAM等のメモリ12上に確保された擬似PARTIESアプリケーションエリア26にコピーし、PARTIESパーティションへの書き込み保護を実現している。この実施の形態2では、ホストプロテクティッドエリア22に確保された領域に擬似PARTIESアプリケーションエリア26をコピーすることで、書き込み保護を実現している。尚、実施の形態1と同様の機能については、同様の符号を用い、ここではその詳細な説明を省略する。

【0035】

図4は、実施の形態2におけるコンピュータシステムの全体構成を示した図である。ハードウェア10の構成で、図1に示したメモリ12をPARTIESアプリケーション23のコピーに用いていないことから、図4ではメモリ12が除かれている。また、ソフトウェア20の構成では、擬似PARTIESアプリケーションエリア26をホストプロテクティッドエリア22の空き領域にコピーしている点が異なる。かかる構成の違いによって、PARTIESアプリケーションアクセスモジュール25の役割として、図1にて説明した、PARTIESアプリケーション23をメモリ12にコピーし、擬似PARTIESアプリケーションエリア26を作る役割の代わりに、PARTIESアプリケーション23をホストプロテクティッドエリア22の空き領域にコピーし、擬似PARTIESアプリケーションエリア26を作る役割を担っている。

【0036】

次に、PARTIESのパーティションにおける書き込み保護について説明する。

図5は、実施の形態2における書き込み保護方法を説明するための図である。

ここでは、ブートが行われる場合、プロテクションされているセキュアなエリアであるPARTIESパーティションを有するHDD11に対して、BIOS21からINT40(Interrupt40)に則ってディスクアクセスが実行される。図2に示す例と同様に、このPARTIESパーティションに、ヘッダであるBERと、PARTIESアプリケーションとしてPSA0～PSA5とが格納されている。このPARTIESパーティションには、アプリケーションに使用している領域とともに、アプリケーションに使用していない領域(空き領域)がある。

【0037】

実施の形態2では、このアプリケーションに使用していない領域を利用して、そこに実行しようとするアプリケーションを全てコピーし、このコピー部分に対してINT40によってアクセスする。図5に示す例では、アプリケーションのPSA3を書き込み保護を必要としない別のPARTIESパーティションにコピーし(PSA3')、ディスクアクセスプログラムのアクセステーブルを変更して、ディスクアクセスプログラムのアクセス範囲をコピーしたエリアに向けるように構成し、このコピーしたエリアに対して、リードやライトを実行するようにした。即ち、ディスクアクセスプログラムのアクセステーブルには、スタートとしてホストプロテクティッドエリア22におけるPSA3'のスタートアドレス、エンドとしてホストプロテクティッドエリア22におけるPSA3'のエンドアドレスが格納されている。これによって、リードもライトも、ホストプロテクティッドエリア22の空き領域に形成された擬似PARTIESアプリケーションエリア26のPSA3'となるように変更される。これによって、擬似的なディスクスペースにアクセスし、オリジナルのPSA3の書き込みを制限すること、即ち、PARTIESパーティションへの書き込み保護を実現している。

【0038】

図6は、実施の形態2におけるPARTIESアプリケーションのブートの流れを示したフローチャートである。PARTIESアプリケーションのブートを実行するに際して(ステップ201)、まず、BIOS21は、ホストプロテクティッドエリア22をアンロックし(ステップ202)、BIOS21は、ホストプ

ロテクティッドエリア22のアクセス機能(ディスクアクセスプログラム)を用意する(ステップ203)。次に、BIOS21は、PARTIESアプリケーション23の承認(Validation)を行う。即ち、物主による承認(例えばHash値による承認)を受ける(ステップ204)。そして、BIOS21は、ホストプロテクティッドエリア22をロックする(ステップ205)。ここで、BIOS21では、承認されたアプリケーションか否かの判断がなされる(ステップ206)。承認されたアプリケーションではない場合には、BIOS21は、エラーを表示し、ブートを失敗させる(ステップ207)。ステップ206で承認されたアプリケーションである場合には、ステップ208に移行する。

【0039】

PARTIESアプリケーションアクセスモジュール25は、PARTIESアプリケーション23のライトプロテクト(Write Protect)が必要かどうかを検出する(ステップ208)。次に、PARTIESアプリケーションアクセスモジュール25では、PARTIESアプリケーション23のサイズ検出がなされる(ステップ209)。ここで、PARTIESアプリケーションアクセスモジュール25は、BIOS21にホストプロテクティッドエリア22のアンロックを要求する(ステップ210)。その後、PARTIESアプリケーションアクセスモジュール25は、ホストプロテクティッドエリア22の空き領域に擬似PARTIESアプリケーションエリア26を作る(ステップ211)。

【0040】

次に、PARTIESアプリケーションアクセスモジュール25は、PARTIESアプリケーション23を読み込み(ステップ212)、ホストプロテクティッドエリア22に確保された擬似PARTIESアプリケーションエリア26に、このPARTIESアプリケーション23をコピーする(ステップ213)。そして、PARTIESアプリケーションアクセスモジュール25は、ホストプロテクティッドエリア22にコピーされた擬似PARTIESアプリケーションエリア26に対するアクセス機能(ディスクアクセスプログラム)を用意し、BIOS21によって用意されたディスクアクセスプログラムと入れ替える(ステップ214)。その後、BIOS21は、ブートのための最初のコードであるイニシ

ヤルプログラムローダを擬似PARTIESアプリケーションエリア26から読み込み(ステップ215)、BIOS21によるPARTIESアプリケーション23のブートが実行される(ステップ216)。

【0041】

このように、実施の形態2では、PARTIESパーティションに導入されているアプリケーション(PARTIESアプリケーション23)を実行する場合に、このアプリケーションの導入されているPARTIESパーティションを、一度、書き込み保護を必要としない別のPARTIESパーティションにコピーするように構成した。そして、元の領域に対するアクセスを、コピーした領域に対する領域に対するアクセスとなるように変更した。より具体的には、図5に示すように、アプリケーションに対するアクセステーブルのアドレスを、擬似PARTIESアプリケーションエリア26のアドレスをコピー先のアドレスとなるように変更した。これによって、元の領域に対するアクセスを無くすことができ、書き込み保護を行いたいPARTIESのパーティションにおける保護を実現している。

【0042】

以上、詳述したように、これらの実施の形態によれば、PARTIESパーティションにおける書き込み制限を実現し、通常のアプリケーションをPARTIESパーティション用のアプリケーションとして使用することができる。このとき、PARTIESパーティション用にアプリケーションを変更し、開発する必要はない。即ち、PARTIESパーティション上のアプリケーション側で問題を解消しなくとも、書き込み制限を行うことが可能となる。また、予期しない書き込みに対する対応が不要となり、更に、PARTIESの仕様の利用範囲を拡張することが可能となる。

【0043】

【発明の効果】

このように、本発明によれば、例えばHDD等の記憶装置において、ユーザから隠蔽された領域に格納されたアプリケーションに対する書き込み保護を実現することができる。

【図面の簡単な説明】

【図1】 実施の形態1におけるコンピュータシステムの全体構成を示した図である。

【図2】 実施の形態1における書き込み保護方法を説明するための図である。

【図3】 実施の形態1におけるPARTIESアプリケーションのブートの流れを示したフローチャートである。

【図4】 実施の形態2におけるコンピュータシステムの全体構成を示した図である。

【図5】 実施の形態2における書き込み保護方法を説明するための図である。

【図6】 実施の形態2におけるPARTIESアプリケーションのブートの流れを示したフローチャートである。

【図7】 HDDにおけるPARTIESの機能を説明するための図である。

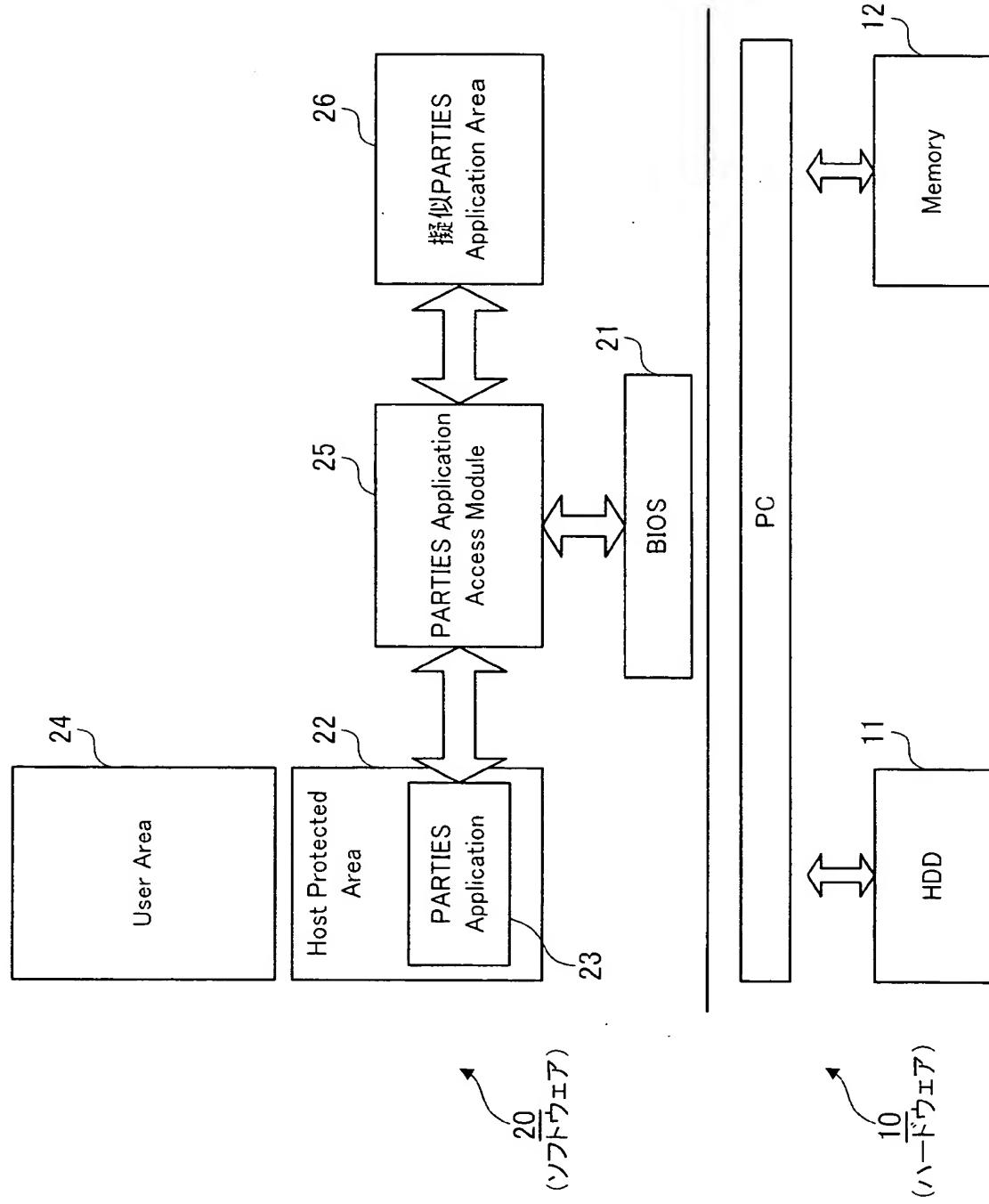
【符号の説明】

1 0…ハードウェア、 1 1…HDD (Hard Disk Drive)、 1 2…メモリ (Memory)、
2 0…ソフトウェア、 2 1…BIOS (Basic Input/Output System)、 2 2…
ホストプロテクティッドエリア (Host Protected Area)、 2 3…PARTIES
アプリケーション (PARTIES Application)、 2 4…ユーザエリア (User Area)、 2
5…PARTIESアプリケーションアクセスモジュール (PARTIES Application
Access Module)、 2 6…擬似PARTIESアプリケーションエリア

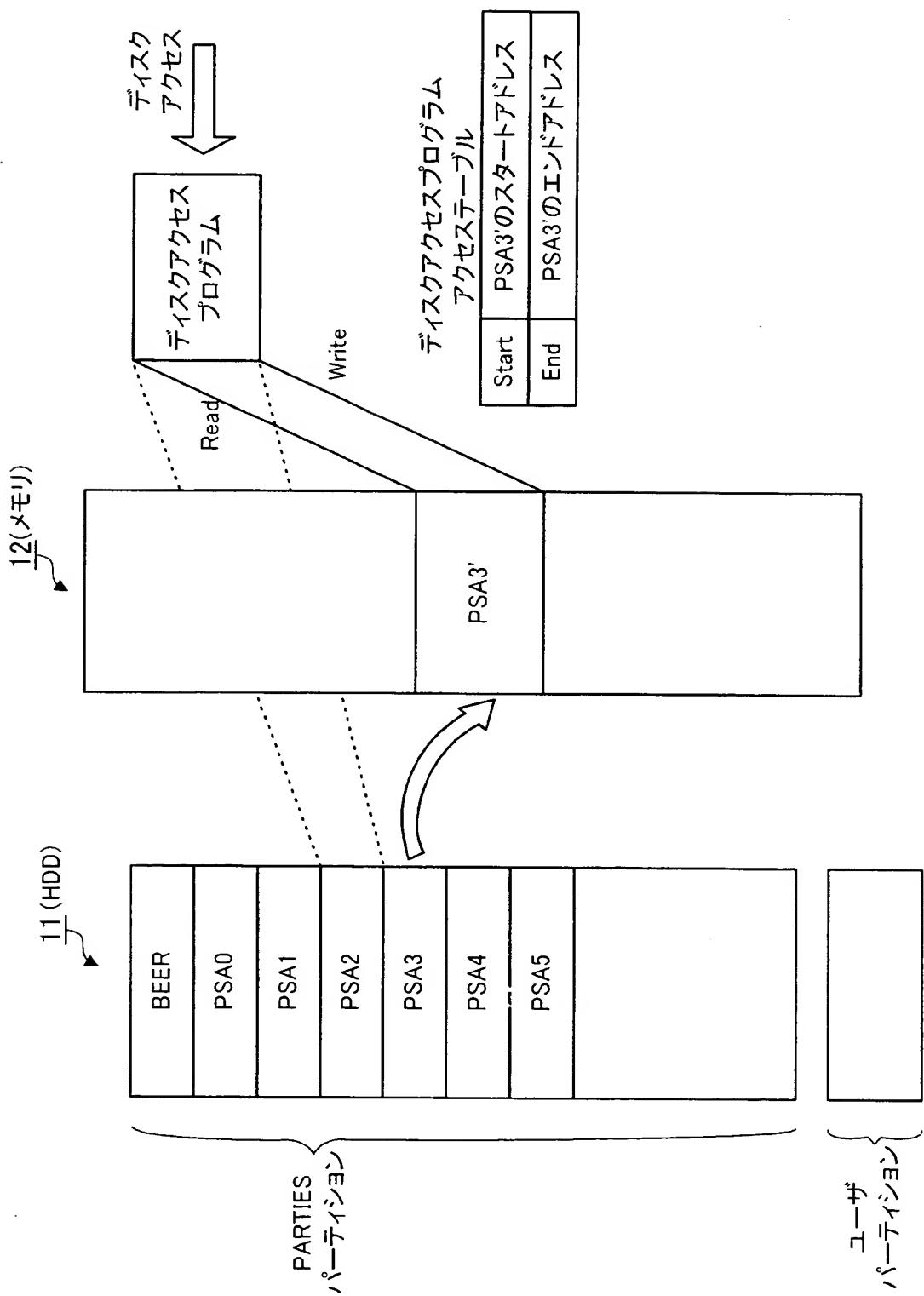
【書類名】

図面

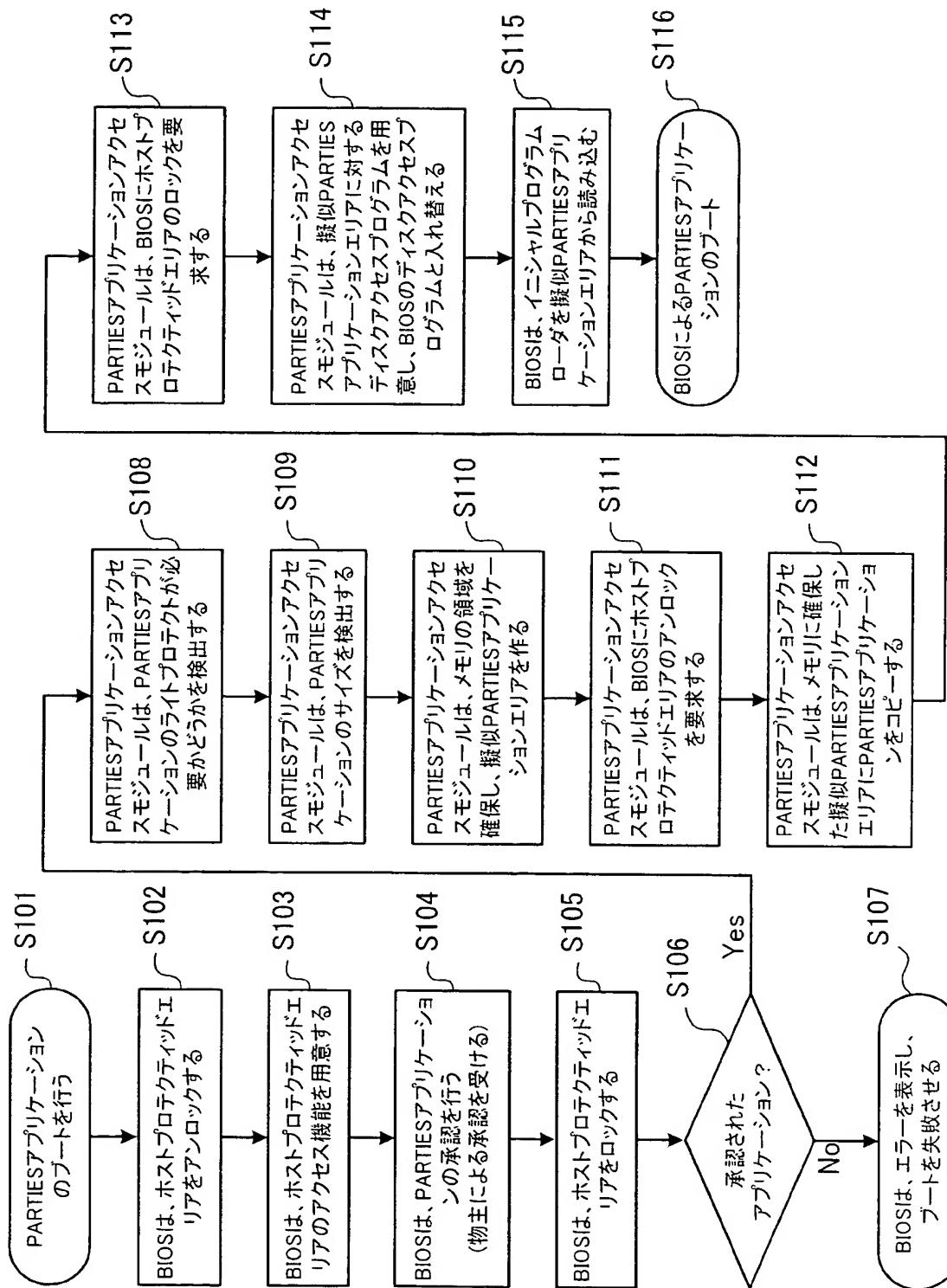
【図 1】



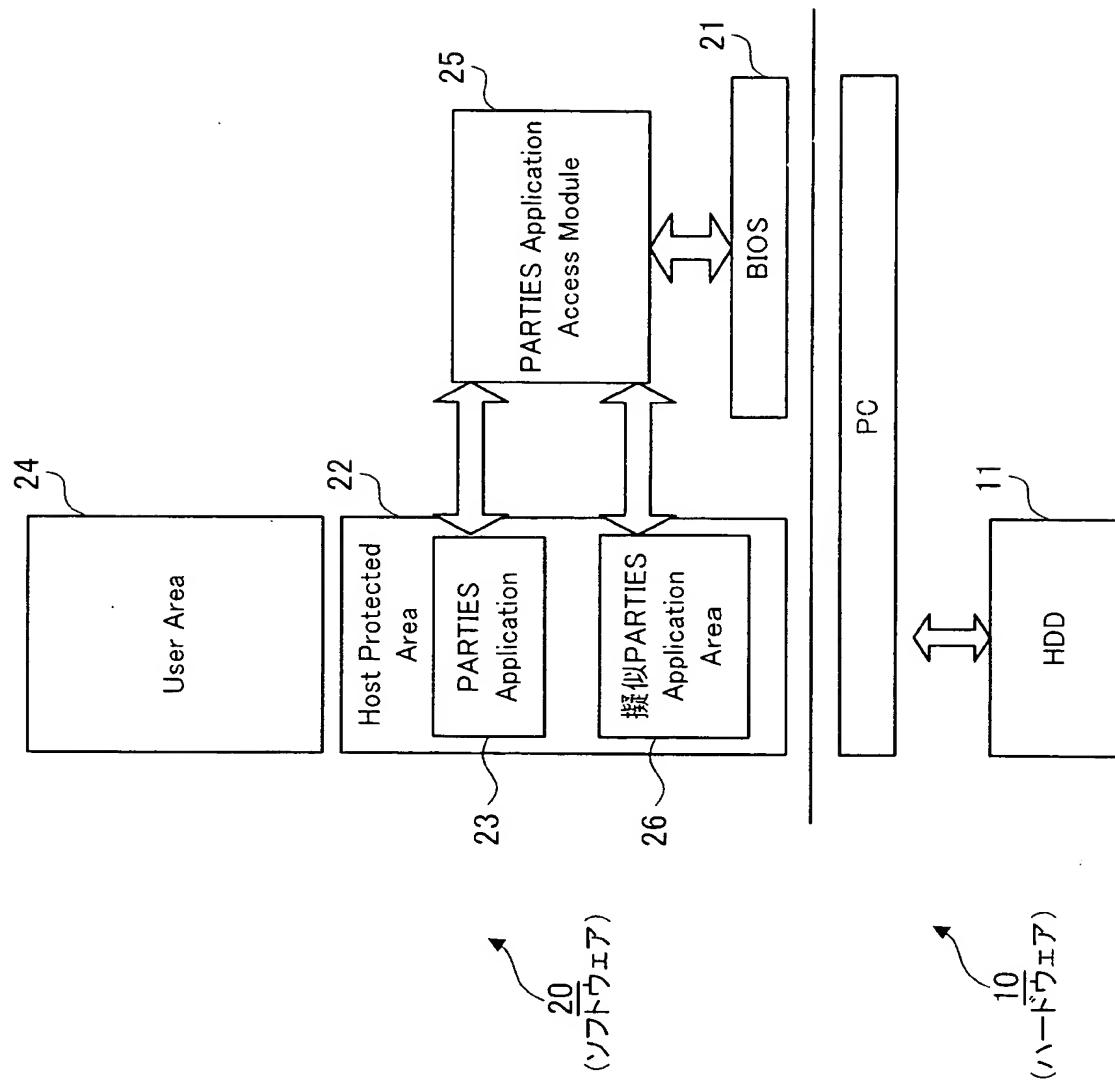
【図 2】



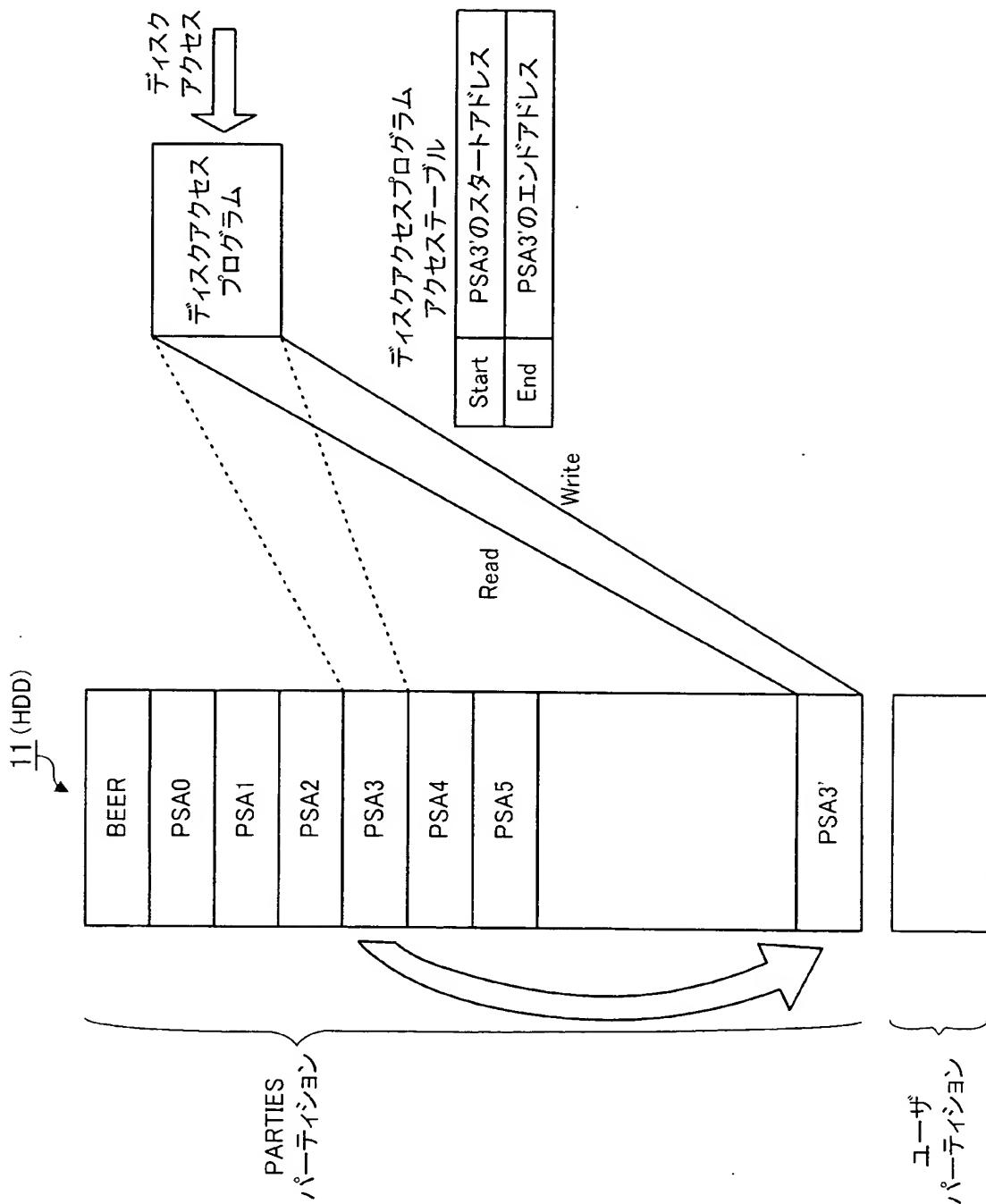
【図 3】



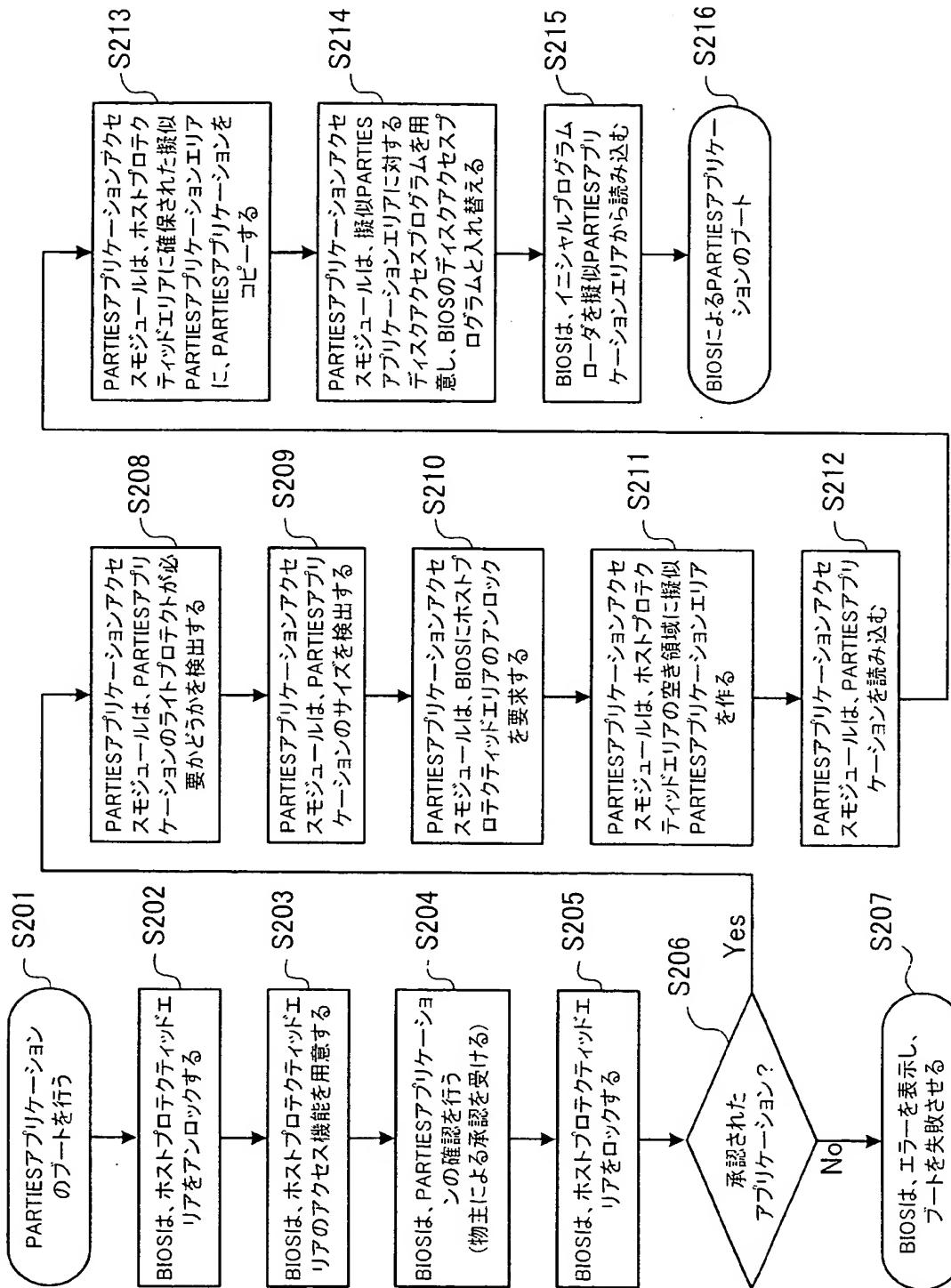
【図 4】



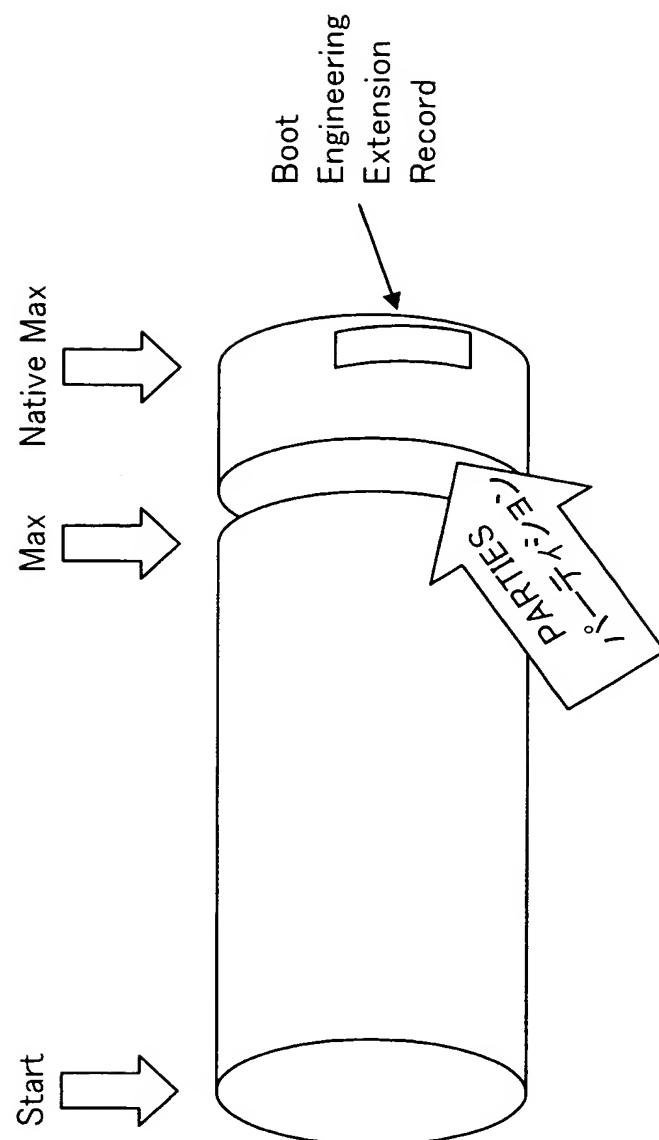
【図 5】



【図 6】



【図7】



【書類名】 要約書

【要約】

【課題】 HDD等の記憶装置において、ユーザから隠蔽された領域に格納されたアプリケーションに対する書き込み保護を実現する。

【解決手段】 ユーザの環境で動作するエリアであるユーザエリア24と、ユーザから保護されたエリアであるホストプロテクティッドエリア22とに区別されてデータを保持するHDD11に対し、ホストプロテクティッドエリア22からのブートをサポートすると共にこのホストプロテクティッドエリア22にあるPARTIESアプリケーション23に対する物主証明のための承認をサポートするBIOS21と、PARTIESアプリケーション23をメモリ12の空き領域にコピーして擬似PARTIESアプリケーションエリア26を生成するPARTIESアプリケーションアクセスモジュール25とを備えた。

【選択図】 図1

認定・付加情報

特許出願の番号	特願 2003-018309
受付番号	50300129764
書類名	特許願
担当官	土井 恵子 4264
作成日	平成 15 年 3 月 10 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	390009531
【住所又は居所】	アメリカ合衆国 10504、ニューヨーク州 アーモンク ニュー オーチャード ロード
【氏名又は名称】	インターナショナル・ビジネス・マシンズ・コーポレーション

【代理人】

【識別番号】	100086243
【住所又は居所】	神奈川県大和市下鶴間 1623 番地 14 日本アイ・ビー・エム株式会社 大和事業所内
【氏名又は名称】	坂口 博

【代理人】

【識別番号】	100091568
【住所又は居所】	神奈川県大和市下鶴間 1623 番地 14 日本アイ・ビー・エム株式会社 大和事業所内
【氏名又は名称】	市位 嘉宏

【代理人】

【識別番号】	100108501
【住所又は居所】	神奈川県大和市下鶴間 1623 番 14 日本アイ・ビー・エム株式会社 知的所有権
【氏名又は名称】	上野 剛史

【復代理人】

【識別番号】	100104880
【住所又は居所】	東京都港区赤坂 5-4-11 山口建設第 2 ビル 6 F セリオ国際特許事務所
【氏名又は名称】	古部 次郎

【選任した復代理人】

【識別番号】	100118201
--------	-----------

次頁有

認定・付力の青幸良（続巻）

【住所又は居所】 東京都港区赤坂5-4-11 山口建設第二ビル
6F セリオ国際特許事務所
【氏名又は名称】 千田 武

次頁無

出証特2003-3099608

特願 2003-018309

出願人履歴情報

識別番号	[390009531]
1. 変更年月日	2000年 5月 16日
[変更理由]	名称変更
住 所	アメリカ合衆国 10504、ニューヨーク州 アーモンク (番地なし)
氏 名	インターナショナル・ビジネス・マシンズ・コーポレーション
2. 変更年月日	2002年 6月 3日
[変更理由]	住所変更
住 所	アメリカ合衆国 10504、ニューヨーク州 アーモンク ニュー オーチャード ロード
氏 名	インターナショナル・ビジネス・マシンズ・コーポレーション